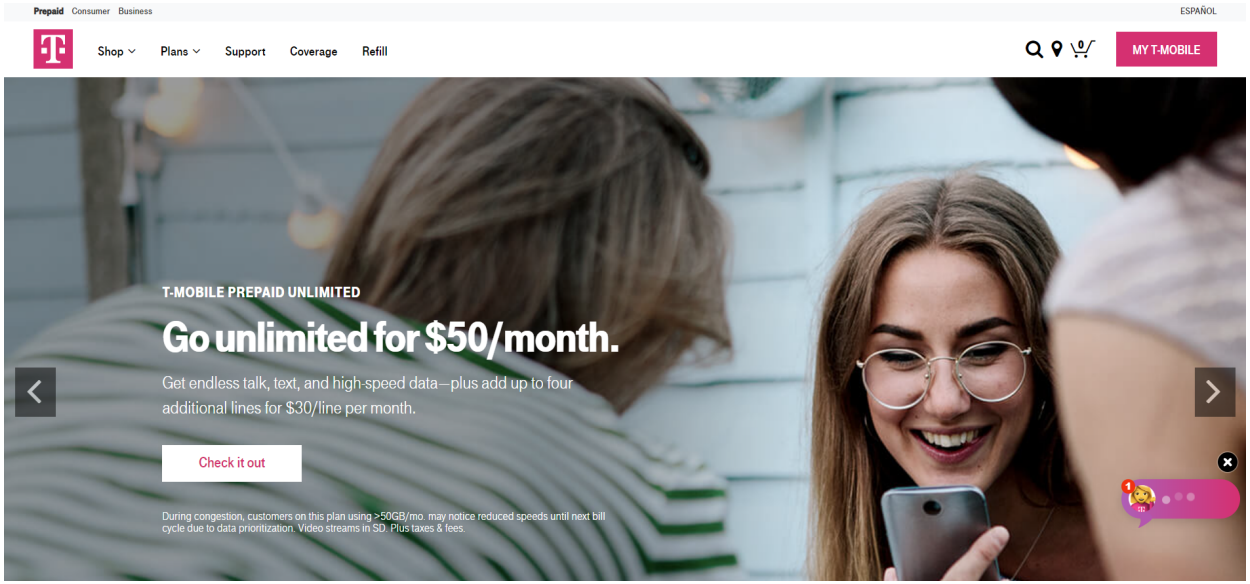
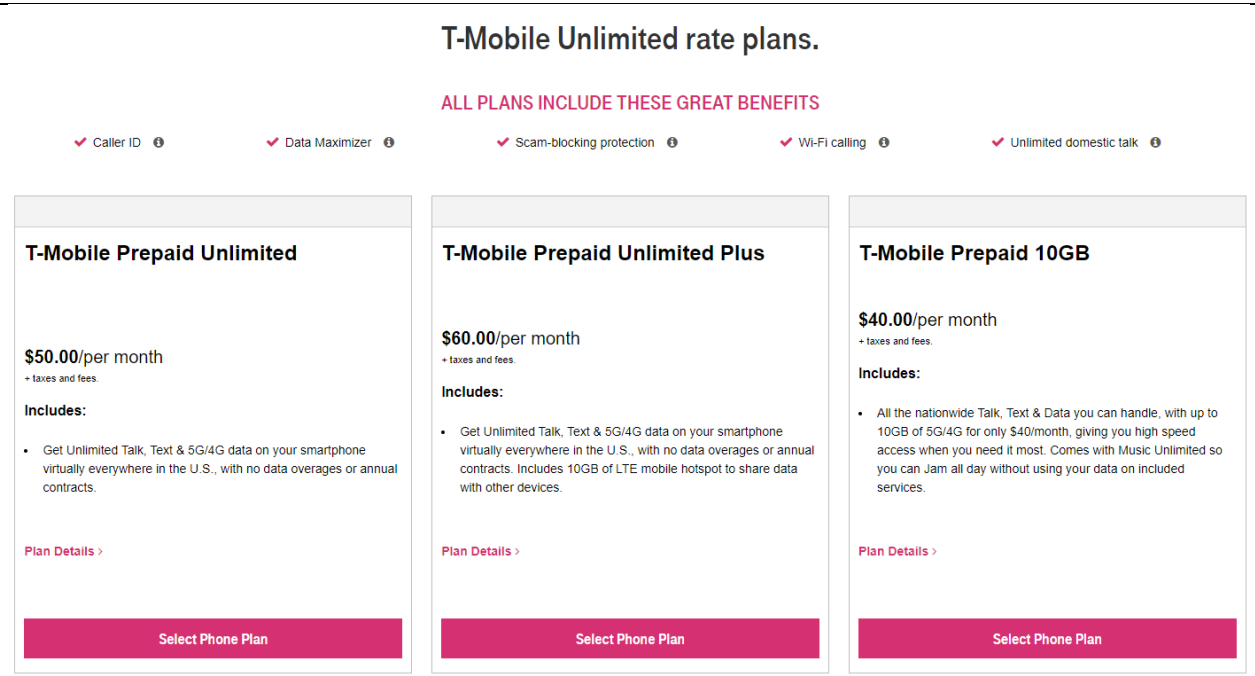
Exhibit H

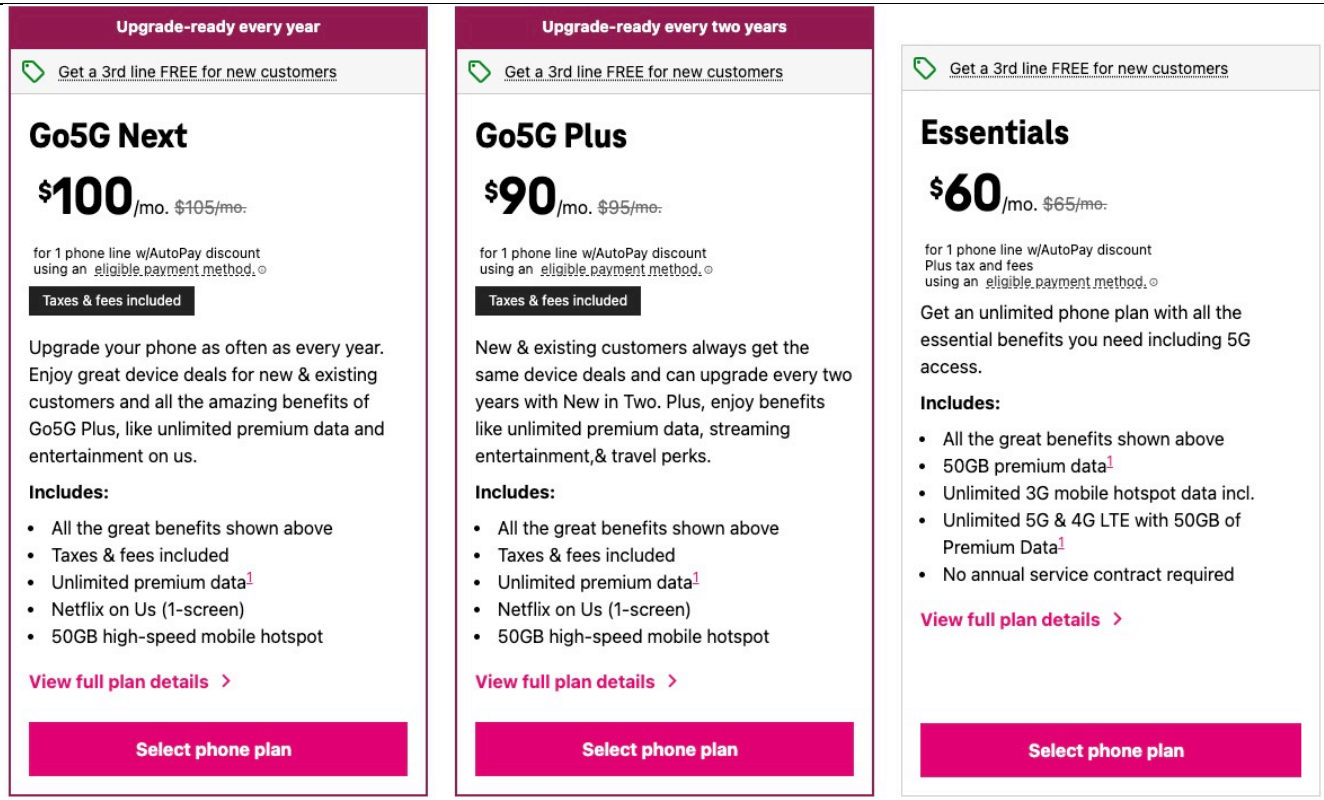
Exhibit H - U.S. Patent No. 9,198,042 ("'042 Patent")

Accused Instrumentalities: smartphones, basic phones, tablets, laptops, and hotspot devices sold (including those sold in bundles with data plans) or used by T-Mobile in conjunction with T-Mobile's servers, hardware, software, and services leased, owned, supported, and/or operated by T-Mobile comprising for use with T-Mobile's wireless network services, and all versions and variations thereof since the issuance of the asserted patent.

Issued Claim(s)	Public Documentation
1. A method comprising:	To the extent the preamble is limiting, T-Mobile's Accused Instrumentalities practice the steps of a method as set forth in the limitations below.
1[a] receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state;	The Accused Instrumentalities comprise receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state. T-Mobile offers telecommunications service plans to customers that are provided through various network elements such as telecommunications base stations and cell sites, edge servers, and other telecommunications servers. T-Mobile provides various network service plans to customers for purchase, including through the T-Mobile.com website as well as through T-Mobile-provided services such as its pre-paid mobile service category, T-Mobile Prepaid Unlimited. *See, e.g.*:  https://prepaid.t-mobile.com/home

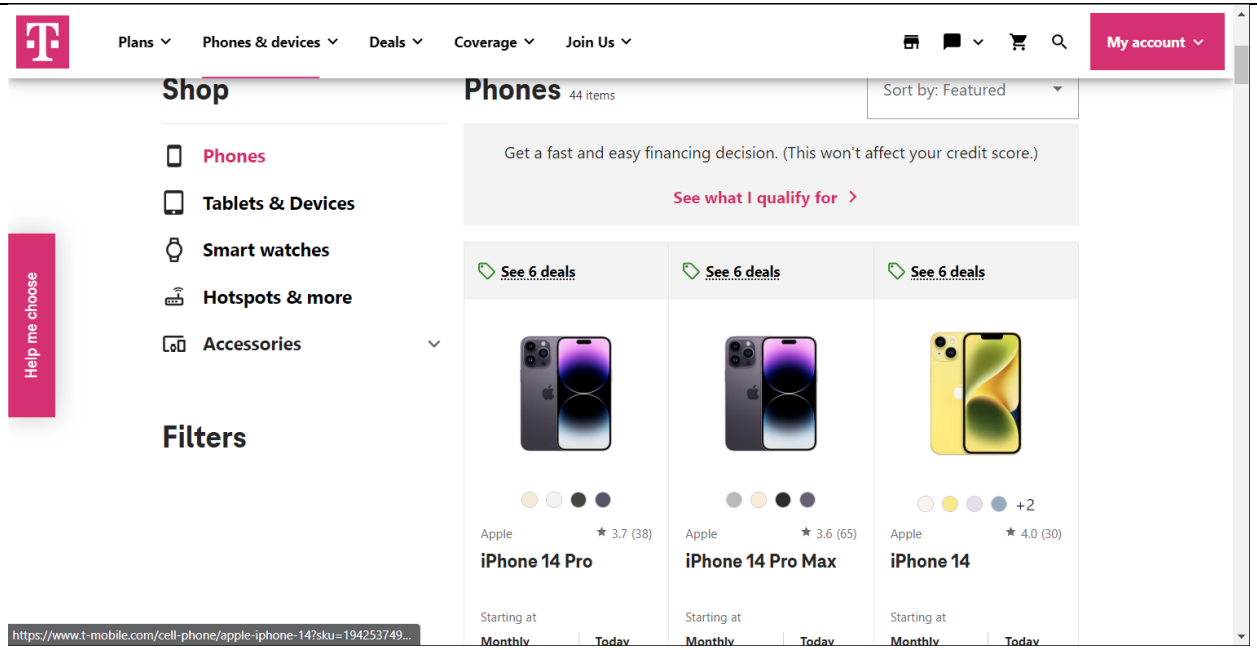


https://prepaid.t-mobile.com/plan-detail/t-mobile-prepaid-plans

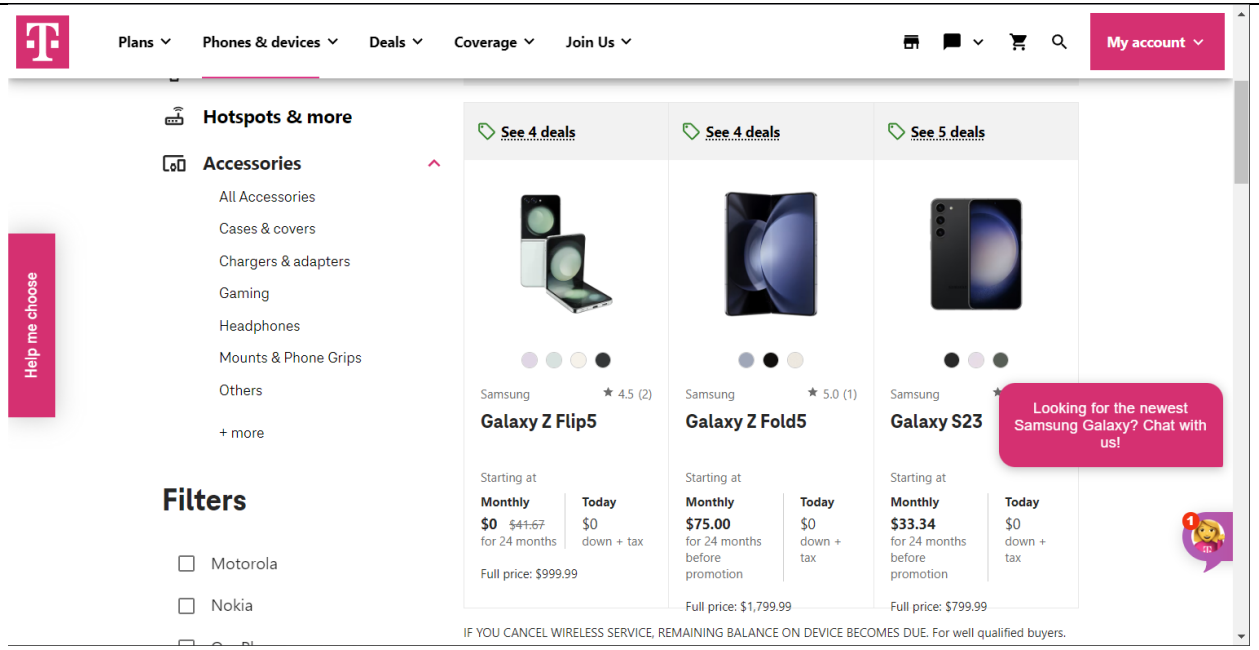


https://www.t-mobile.com/cell-phone-plans

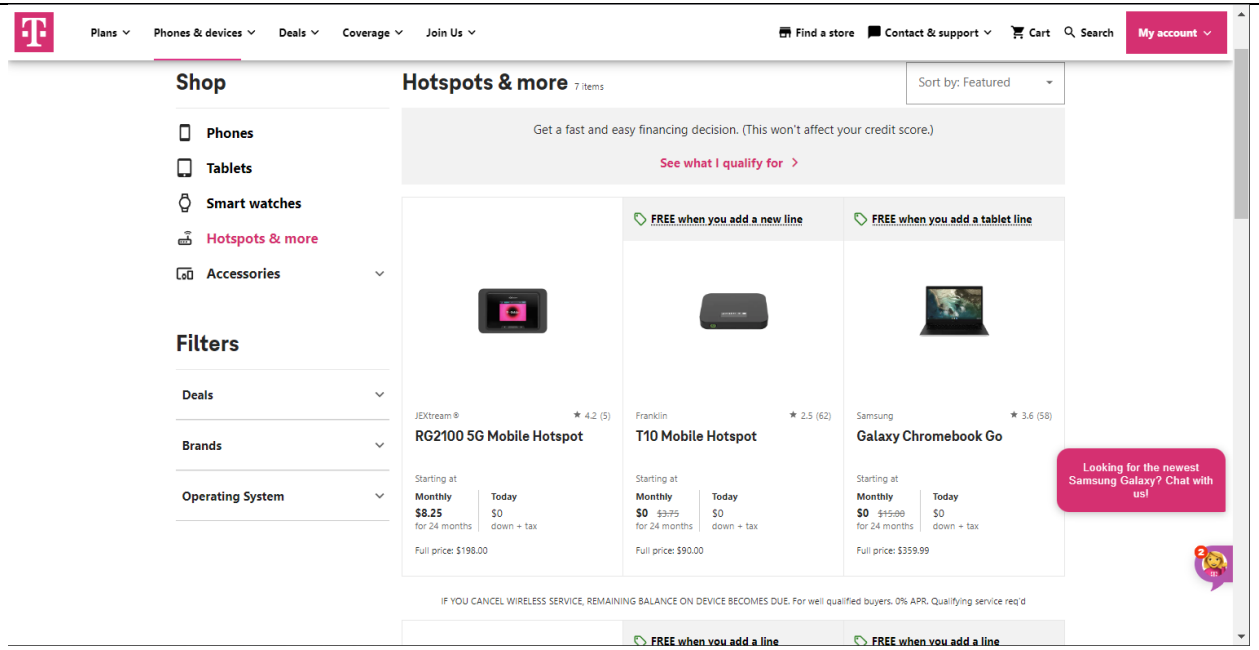
T-Mobile sells mobile devices such as phones, tablets, and hotspot access points which communicate with the T-Mobile wireless service network, which is a wireless access network. Such devices comprise end-user devices, as do devices which customers purchase elsewhere and "bring" to the T-Mobile network. *See, e.g.*:



https://www.t-mobile.com/cell-phones?INTNAV=tNav:Devices:CellPhones



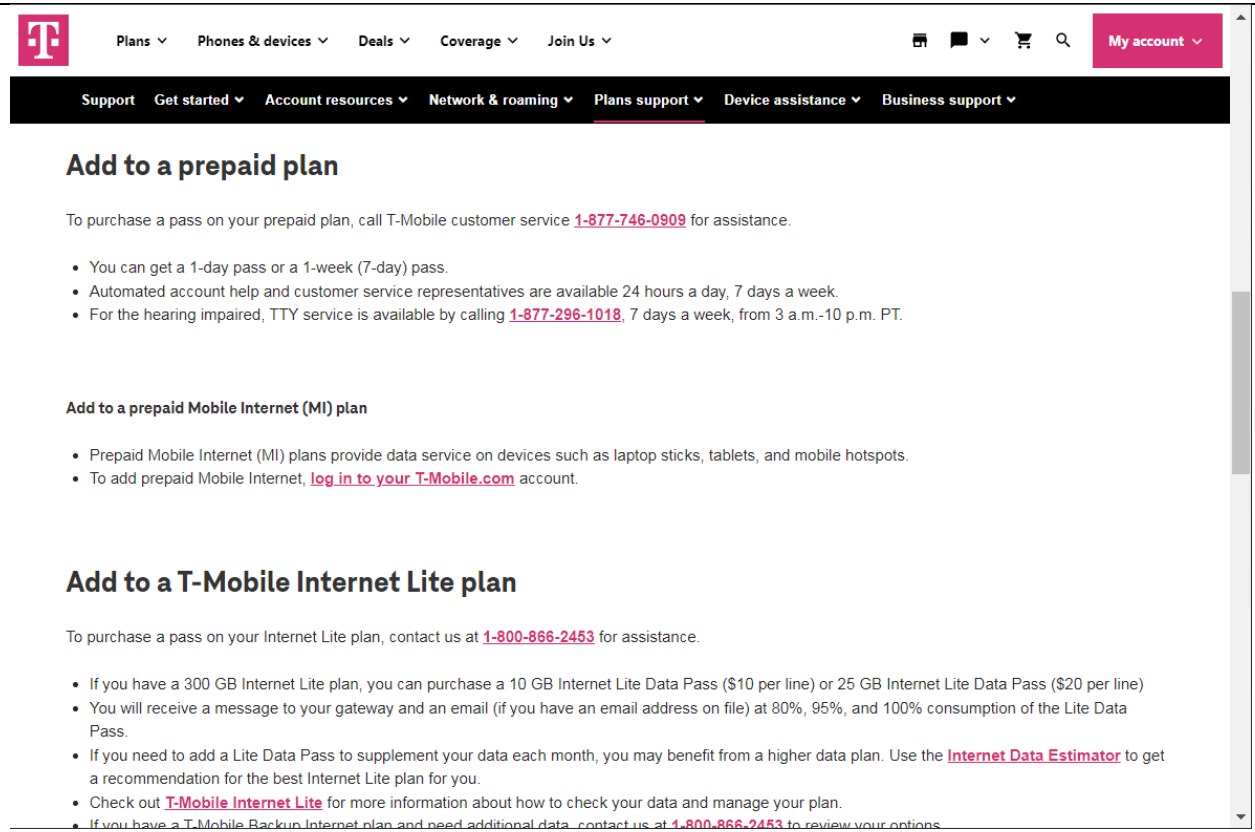
https://www.t-mobile.com/cell-phones/brand/samsung



https://www.t-mobile.com/hotspots-iot-connected-devices

The Accused Instrumentalities use different service plans to provide service, for example, to mobile hotspot devices, mobile phones and tablets provisioned with an "unlimited" data plan, mobile phones and tablets provisioned with a prepaid plan, mobile phones and tablets which for which the associated subscriber account has reached its allotted data limit for the service period, and mobile phones and tablets which are specifically communicating with T-Mobile servers to purchase or increase data allotments (e.g., a T-Mobile "Data Pass").

See, e.g.:



https://www.t-mobile.com/support/plans-features/data-passes#prepaid

Verizon's network receives service plan information from devices which correspond to the subscriber service plan associated with that wireless end-user device, which is a report comprising information about a device service state. For example, Verizon's network receives an attach request, bearer resource allocation request, bearer resource modification request, or PDN connectivity request from a wireless end-user device (UE), which includes a report comprising information about the UE's service state such as UE network capability, UE status, and protocol configuration options (PCO):

Table 8.2.4.1: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach request message identity	Message type 9.8	M	V	1
	EPS attach type	EPS attach type 9.9.3.11	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	EPS mobile identity	EPS mobile identity 9.9.3.12	M	LV	5-12
	UE network capability	UE network capability 9.9.3.34	M	LV	3-14
	ESM message container	ESM message container 9.9.3.15	M	LV-E	5-n
19	Old P-TMSI signature	P-TMSI signature 9.9.3.26	O	TV	4
50	Additional GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
52	Last visited registered TAI	Tracking area identity 9.9.3.32	O	TV	6
5C	DRX parameter	DRX parameter 9.9.3.8	O	TV	3
31	MS network capability	MS network capability 9.9.3.20	O	TLV	4-10
13	Old location area identification	Location area identification 9.9.2.2	O	TV	6
9-	TMSI status	TMSI status 9.9.3.31	O	TV	1
11	Mobile station classmark 2	Mobile station classmark 2 9.9.2.4	O	TLV	5
20	Mobile station classmark 3	Mobile station classmark 3 9.9.2.5	O	TLV	2-34
40	Supported Codecs	Supported Codec List 9.9.2.10	O	TLV	5-n
F-	Additional update type	Additional update type 9.9.3.0B	O	TV	1
5D	Voice domain preference and UE's usage setting	Voice domain preference and UE's usage setting 9.9.3.44	O	TLV	3
D-	Device properties	Device properties 9.9.2.0A	O	TV	1
E-	Old GUTI type	GUTI type 9.9.3.45	O	TV	1
C-	MS network feature support	MS network feature support 9.9.3.20A	O	TV	1
10	TMSI based NRI container	Network resource identifier container 9.9.3.24A	O	TLV	4
6A	T3324 value	GPRS timer 2 9.9.3.16A	O	TLV	3
5E	T3412 extended value	GPRS timer 3 9.9.3.16B	O	TLV	3
6E	Extended DRX parameters	Extended DRX parameters 9.9.3.46	O	TLV	3
6F	UE additional security capability	UE additional security capability 9.9.3.53	O	TLV	6
6D	UE status	UE status 9.9.3.54	O	TLV	3
17	Additional information requested	Additional information requested 9.9.3.55	O	TV	2

Table 8.3.8.1: BEARER RESOURCE ALLOCATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource allocation request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
	Required traffic flow QoS	EPS quality of service 9.9.4.3	M	LV	2-14
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

Table 8.3.10.1: BEARER RESOURCE MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource modification request message identity	Message type 9.8	M	V	1
	EPS bearer identity for packet filter	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
5B	Required traffic flow QoS	EPS quality of service 9.9.4.3	O	TLV	3-15
58	ESM cause	ESM cause 9.9.4.4	O	TV	2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

Table 8.3.20.1: PDN CONNECTIVITY REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN connectivity request message identity	Message type 9.8	M	V	1
	Request type	Request type 9.9.4.14	M	V	1/2
	PDN type	PDN type 9.9.4.10	M	V	1/2
D-	ESM information transfer flag	ESM information transfer flag 9.9.4.5	O	TV	1
28	Access point name	Access point name 9.9.4.1	O	TLV	3-102
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538

3GPP TS 24.301 v15.03

Flows

There are three scenarios where the PCO value will be passed to the host:

- When a new PCO value has arrived on an activated connection
- When an app or service queries for the latest PCO value from the modem
- When a connection is bridged or activated for the first time and a PCO value already exists in the modem

For the first scenario, the modem should send an NDIS_STATUS_WWAN_PCO_STATUS notification to the OS indicating a new PCO value change whenever a new PCO value is received from the network, with the appropriate NDIS port number to represent the corresponding PDN. To avoid draining the battery unnecessarily, the modem should avoid noisy notifications, as described in Modem behavior with Selective Suspend and Connected Standby.

For the second scenario, when an app or service queries for PCO value from the modem on an activated PDN connection, the host will send the modem an OID_WWAN_PCO query request to read the latest cached PCO value in the modem.

For the third scenario, when a connection is activated or bridged on the host, the modem should send an **NDIS_STATUS_WWAN_PCO_STATUS** notification when a PCO value already exists in the modem for the activated or bridged connection the host requested. The notification should be passed up from the corresponding NDIS port number of the PDN.

	https://learn.microsoft.com/en-us/windows-hardware/drivers/network/mb-protocol-configuration-options-pco-operations
1[b] determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified, the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting, the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network, the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and	The Accused Instrumentalities comprise "determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified, the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting, the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network, the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network." Examples of such service policy settings on the wireless end-user device include, for example, APN access settings and service plan settings stored on the wireless end-user device, including for example in an encrypted partition of the device or in an encrypted SIM card. Such service policy settings are configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network, insofar as the policies are used by T-Mobile to determine the levels of service that are to be provided to the wireless end-user device. Carrier configuration information (which is service profile information) on a given wireless end-user device is secured within the device through the use of privileges and other access settings, including through the use of matching signatures between the carrier settings and one stored with the SIM card information. *See, e.g.*: **Manually update your carrier settings on your iPhone or iPad** Carrier settings updates let your carrier provider update carrier network and related settings to improve cellular network connectivity and performance. Carrier settings updates can also add support for new features like 5G or Wi-Fi Calling. When a carrier settings update is available, you'll be prompted to install it. Installation takes less than one minute, and you can keep using your device normally. If your carrier releases a mandatory update, you'll see an OK button instead of an Update button to let you know that the update was downloaded and installed. https://support.apple.com/en-us/HT201270

Carrier Configuration

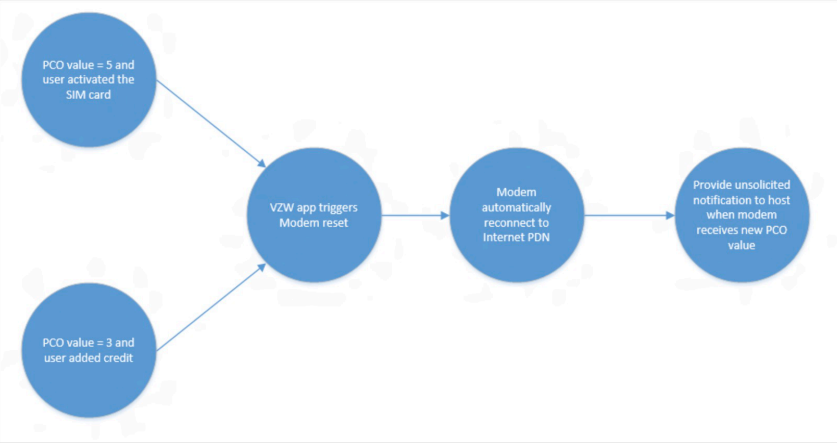
Android 6.0 and higher include a capability for privileged apps to provide carrier-specific configuration to the platform. This functionality, based on the UICC Carrier Privileges introduced in Android 5.1 (Lollipop MR1), allows carrier configuration to be moved away from the static configuration overlays and gives carriers and OEMs the ability to dynamically provide carrier configuration to the platform through a defined interface.

A properly signed carrier app can either be preloaded in the system image, installed automatically, or manually installed through an app store. The app is queried by the platform to provide configuration for settings including:

- Roaming/nonroaming networks
- Visual voicemail
- SMS/MMS network settings
- VoLTE/IMS configurations

Note: This app must be signed with the certificate that has a matching signature to one on the SIM. See How is privilege granted to a carrier app for details.

https://source.android.com/docs/core/connect/carrier

	Resetting the modem based on PCO values Based on PCO values received from the network, the modem will be reset in the following scenarios: • The user completed self-activation after receiving PCO = 5 from the network. A new PCO value (3, 0 or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App. • The user added more credit to their account after receiving PCO = 3. A new PCO value (0, or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App. The host is not aware of the modem being reset, so the activated connections from the host will not be deactivated and the modem should automatically re-establish connection with those PDN after resetting. Upon establishing connection and receiving a new incoming PCO value from the network, the modem will provide an unsolicited NDIS_STATUS_WWAN_PCO_STATUS notification to the host. The following diagram illustrates the modem's reset flow when one of these scenarios occurs, with Verizon Wireless as the example MO:  https://learn.microsoft.com/en-us/windows-hardware/drivers/network/mb-protocol-configuration-options-pco-operations
1[c] in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing	The Accused Instrumentalities comprise receiving a report comprising device service states "in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting." T-Mobile's network makes determinations that particular service policies for user devices need to be changed when, for example, a subscriber's service plan is changed or service-related options are activated or deactivated (e.g., the "Data Pass" option or "HD Streaming" option).

modifications to the particular service policy setting.	On information and belief, the Accused Instrumentalities specifically transmit traffic control-related instructions to mobile devices in the wireless access network based on type of traffic, type of subscriber plan, and priority levels for types of data and/or subscriber account type based on the Accused Instrumentalities' inspection of traffic to and from the device and the account associated with the device. For example, the Accused Instrumentalities inspect data traffic to determine if it is for streaming video to devices, and manages data access by that device accordingly. *See, e.g.*:

Activation steps

If you don't have a plan that includes HD streaming, refer to **Find the right plan for you** to add a plan today.

From the T-Mobile app

1. Open the T-Mobile app. If you don't have it, **learn how to download it now**.
2. Tap **MORE**
3. Go to **PROFILE SETTINGS**
4. Go to **MEDIA SETTINGS**.
5. If you have multiple lines on your account, make sure the line you're making changes to is showing. If it's not, open the menu to select another line on the account.
6. Next to **HD Video Resolution**, toggle it **ON** or **OFF**.

From T-Mobile.com

1. **Log in to T-Mobile.com** with your T-Mobile ID. If you don't have one, **register for a T-Mobile ID**.
2. Select **PROFILE**.
3. Go to **MEDIA SETTINGS**.
4. By **HD Video Resolution**, set the option to **ON** or **OFF**.

HD video resolution details

- Activating HD video resolution only provides the ability to enable higher-resolution video streams by turning off video optimization. It doesn't change the actual, available resolution of streaming video.
- Video resolution isn't determined by T-Mobile, but rather it's determined by the video content provider like YouTube or Netflix.
- Once you turn it on, HD video streaming availability should take effect immediately, but it may require closing and re-opening the app or browser window, or restarting your device.

Full terms

All on-network data used, including free streaming data, counts toward the heavy-user threshold of 50GB in a billing cycle, after which a T-Mobile-branded customer will no longer receive highest priority on the network. When an HD video is active, streaming high-definition video will use data much faster than optimized video, and brings up to the possibility of de-prioritization if you use enough data to reach that limit in a given month. (Learn more about T-Mobile's **Open Internet** disclosures.)

	https://www.t-mobile.com/support/plans-features/activate-hd-video-streaming **Unlimited video streaming with Binge On™** As a Simple Choice™ customer, you can stream all the video you want while on our network. Data charges do not apply. During congestion, heavy data users (>50GB/mo. for most plans) and customers choosing lower-prioritized plans may notice lower speeds than other customers. https://www.t-mobile.com/tv-streaming/binge-on **Manually update your carrier settings on your iPhone or iPad** Carrier settings updates let your carrier provider update carrier network and related settings to improve cellular network connectivity and performance. Carrier settings updates can also add support for new features like 5G or Wi-Fi Calling. When a carrier settings update is available, you'll be prompted to install it. Installation takes less than one minute, and you can keep using your device normally. If your carrier releases a mandatory update, you'll see an OK button instead of an Update button to let you know that the update was downloaded and installed. https://support.apple.com/en-us/HT201270

Carrier Configuration

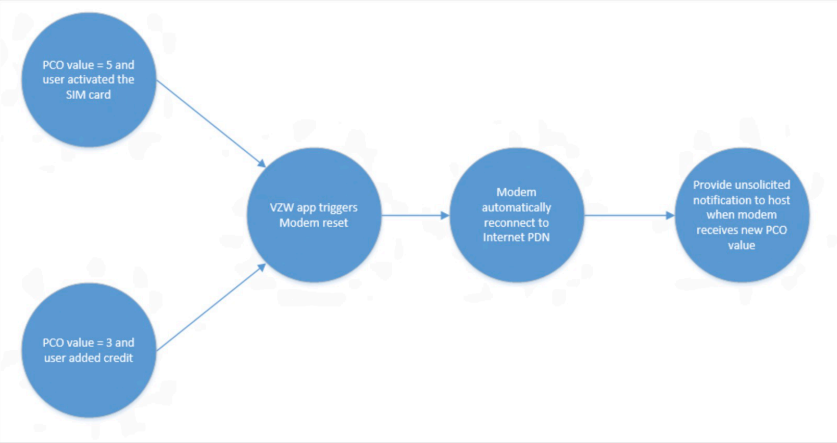
Android 6.0 and higher include a capability for privileged apps to provide carrier-specific configuration to the platform. This functionality, based on the UICC Carrier Privileges introduced in Android 5.1 (Lollipop MR1), allows carrier configuration to be moved away from the static configuration overlays and gives carriers and OEMs the ability to dynamically provide carrier configuration to the platform through a defined interface.

A properly signed carrier app can either be preloaded in the system image, installed automatically, or manually installed through an app store. The app is queried by the platform to provide configuration for settings including:

- Roaming/nonroaming networks
- Visual voicemail
- SMS/MMS network settings
- VoLTE/IMS configurations

Note: This app must be signed with the certificate that has a matching signature to one on the SIM. See How is privilege granted to a carrier app for details.

https://source.android.com/docs/core/connect/carrier

	Resetting the modem based on PCO values Based on PCO values received from the network, the modem will be reset in the following scenarios: • The user completed self-activation after receiving PCO = 5 from the network. A new PCO value (3, 0 or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App. • The user added more credit to their account after receiving PCO = 3. A new PCO value (0, or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App. The host is not aware of the modem being reset, so the activated connections from the host will not be deactivated and the modem should automatically re-establish connection with those PDN after resetting. Upon establishing connection and receiving a new incoming PCO value from the network, the modem will provide an unsolicited NDIS_STATUS_WWAN_PCO_STATUS notification to the host. The following diagram illustrates the modem's reset flow when one of these scenarios occurs, with Verizon Wireless as the example MO:  https://learn.microsoft.com/en-us/windows-hardware/drivers/network/mb-protocol-configuration-options-pco-operations
2. The method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control.	The Accused Instrumentalities comprise the particular service policy setting assists in implementing a roaming control. On information and belief, the protocol configuration options information assists in modifying the service policy setting which controls cellular communications, including when the mobile device is roaming. *See, e.g.*:

Carrier Configuration

Android 6.0 and higher include a capability for privileged apps to provide carrier-specific configuration to the platform. This functionality, based on the UICC Carrier Privileges introduced in Android 5.1 (Lollipop MR1), allows carrier configuration to be moved away from the static configuration overlays and gives carriers and OEMs the ability to dynamically provide carrier configuration to the platform through a defined interface.

A properly signed carrier app can either be preloaded in the system image, installed automatically, or manually installed through an app store. The app is queried by the platform to provide configuration for settings including:

- Roaming/nonroaming networks
- Visual voicemail
- SMS/MMS network settings
- VoLTE/IMS configurations

Note: This app must be signed with the certificate that has a matching signature to one on the SIM. See How is privilege granted to a carrier app for details.

https://source.android.com/docs/core/connect/carrier

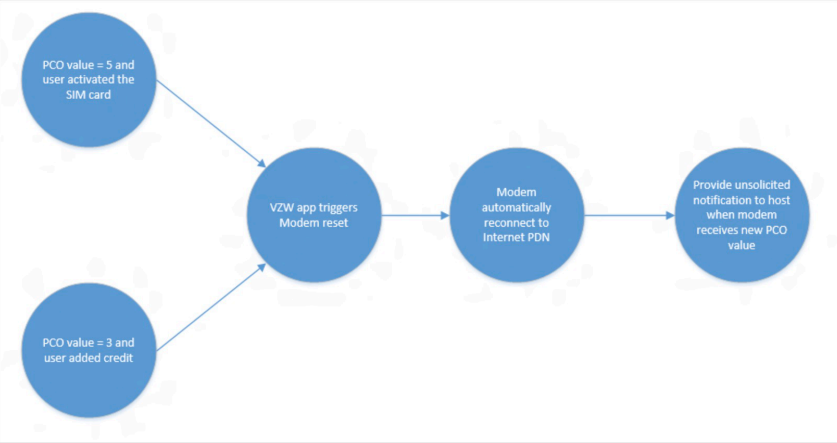
Resetting the modem based on PCO values

Based on PCO values received from the network, the modem will be reset in the following scenarios:

- The user completed self-activation after receiving PCO = 5 from the network. A new PCO value (3, 0 or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App.
- The user added more credit to their account after receiving PCO = 3. A new PCO value (0, or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App.

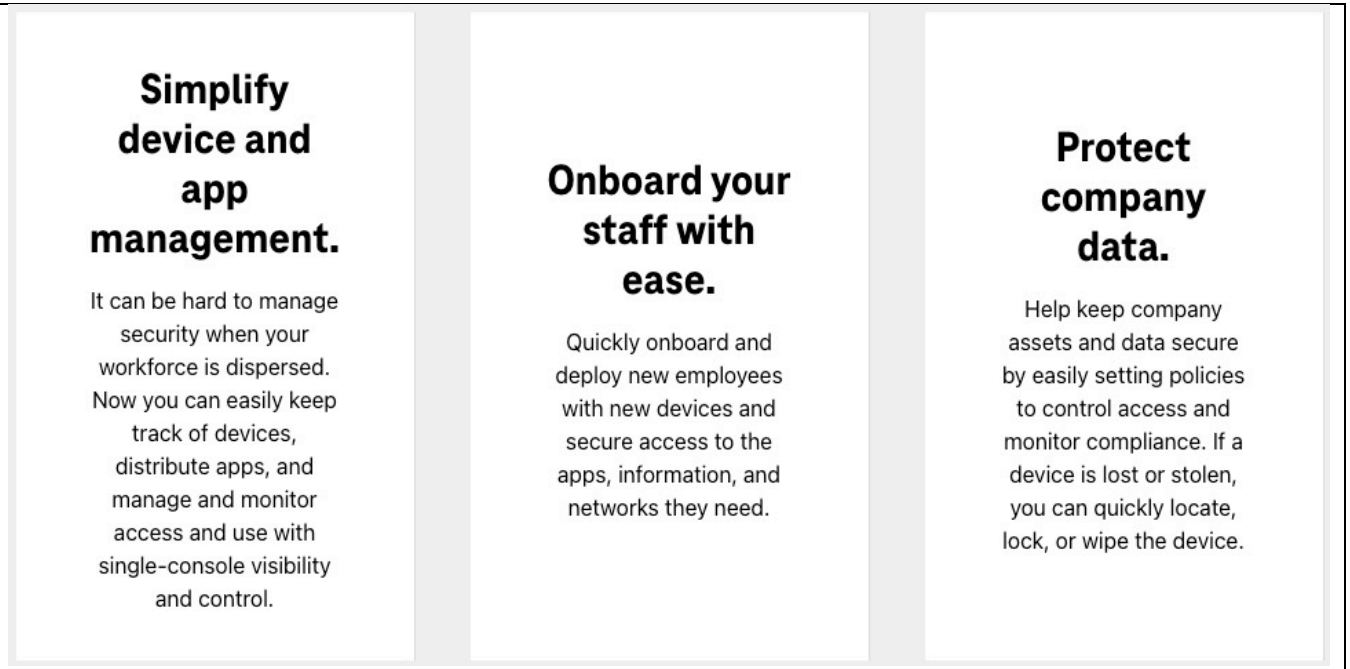
The host is not aware of the modem being reset, so the activated connections from the host will not be deactivated and the modem should automatically re-establish connection with those PDN after resetting. Upon establishing connection and receiving a new incoming PCO value from the network, the modem will provide an unsolicited NDIS_STATUS_WWAN_PCO_STATUS notification to the host.

The following diagram illustrates the modem's reset flow when one of these scenarios occurs, with Verizon Wireless as the example MO:



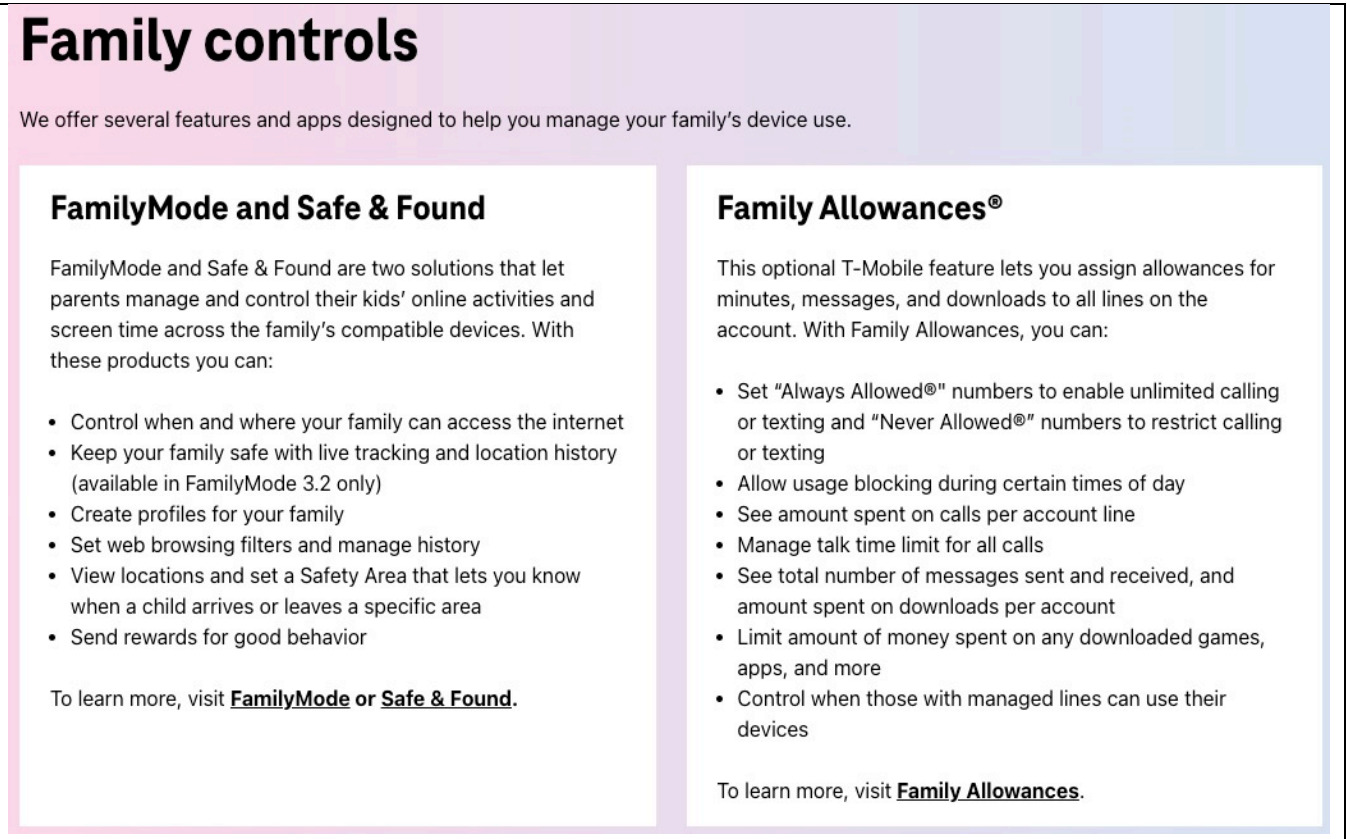
https://learn.microsoft.com/en-us/windows-hardware/drivers/network/mb-protocol-configuration-options-pco-operations

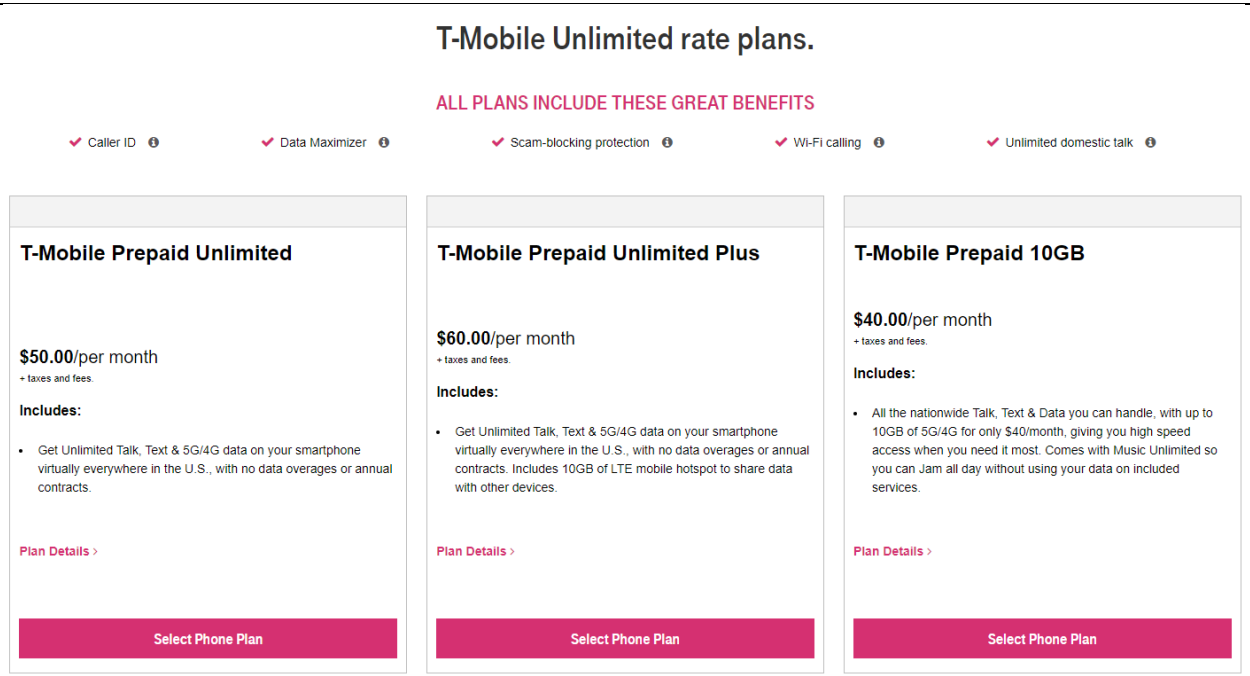
The Accused Instrumentalities comprise the particular service policy setting assists in implementing an enterprise wireless wide-area network (WWAN) management control. On information and belief, the protocol configuration options information assists in modifying the service policy setting which controls cellular communications, including when the mobile device is used in an enterprise. *See, e.g.*:



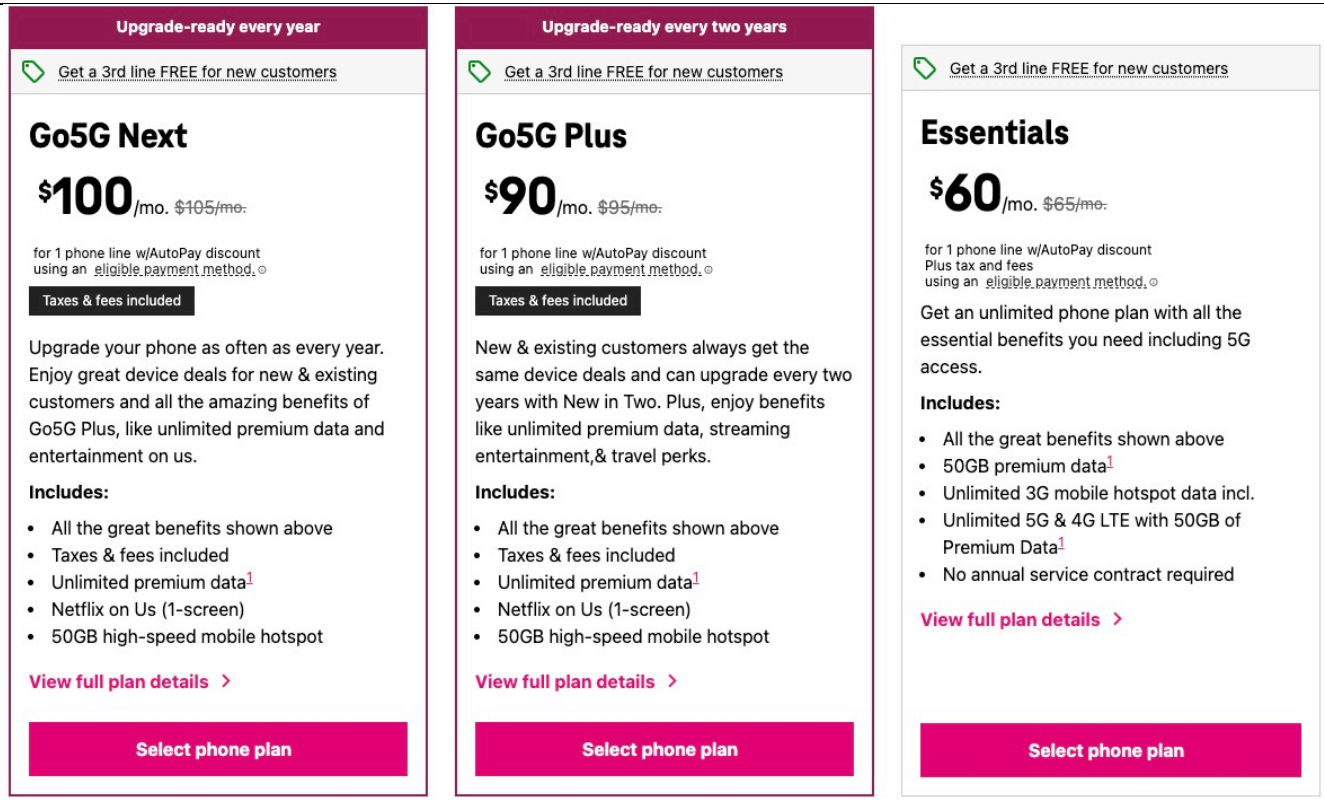
https://www.t-mobile.com/business/solutions/security/mobile-device-management

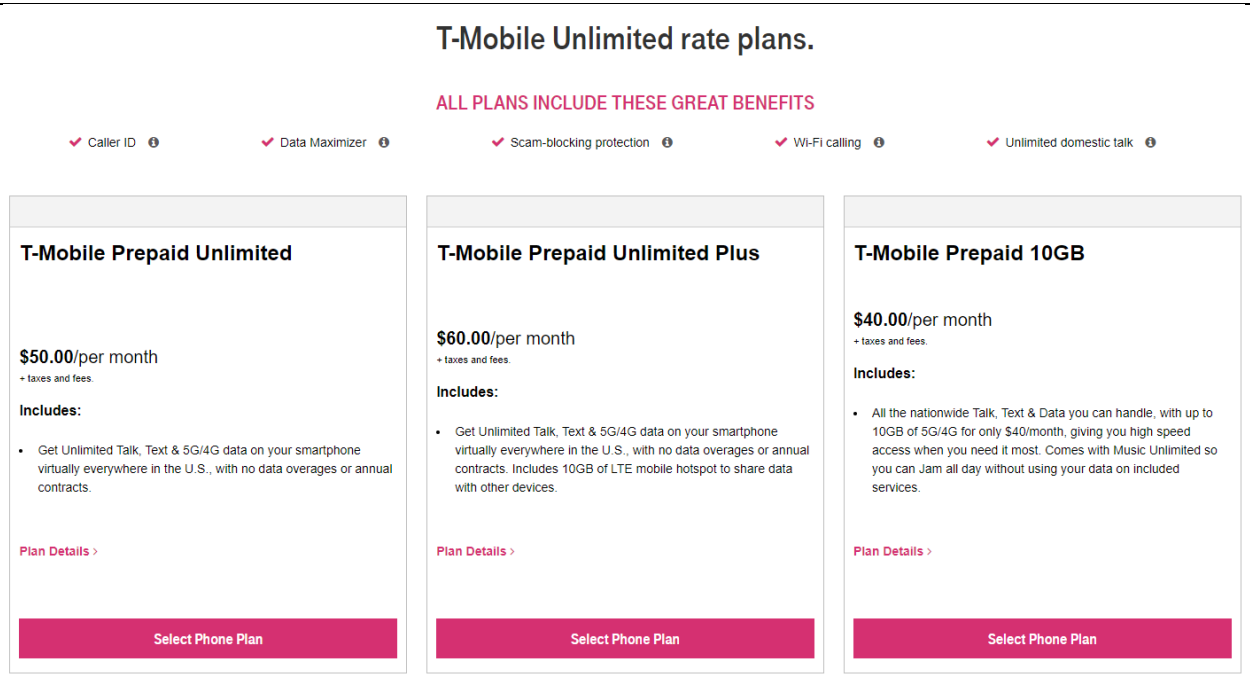
The Accused Instrumentalities comprise the particular service policy setting assists in implementing parental controls. On information and belief, the protocol configuration options information assists in modifying the service policy setting which controls cellular communications, including when the mobile device is used in a family account. *See, e.g.*:

	 https://www.t-mobile.com/privacy-center/education/family-controls
3. The method of claim 1, wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN).	The Accused Instrumentalities comprise sending configuration information to the wireless end-user device wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN). Mobile devices such as phones, tablets, and hotspot access points which communicate with the T-Mobile wireless service network (a wireless wide-area network (WWAN)) and have a mobile hotspot feature are intermediate networking devices that forward traffic between T-Mobile's network (WWAN) and a local WiFi network (WLAN). *See, e.g.*:

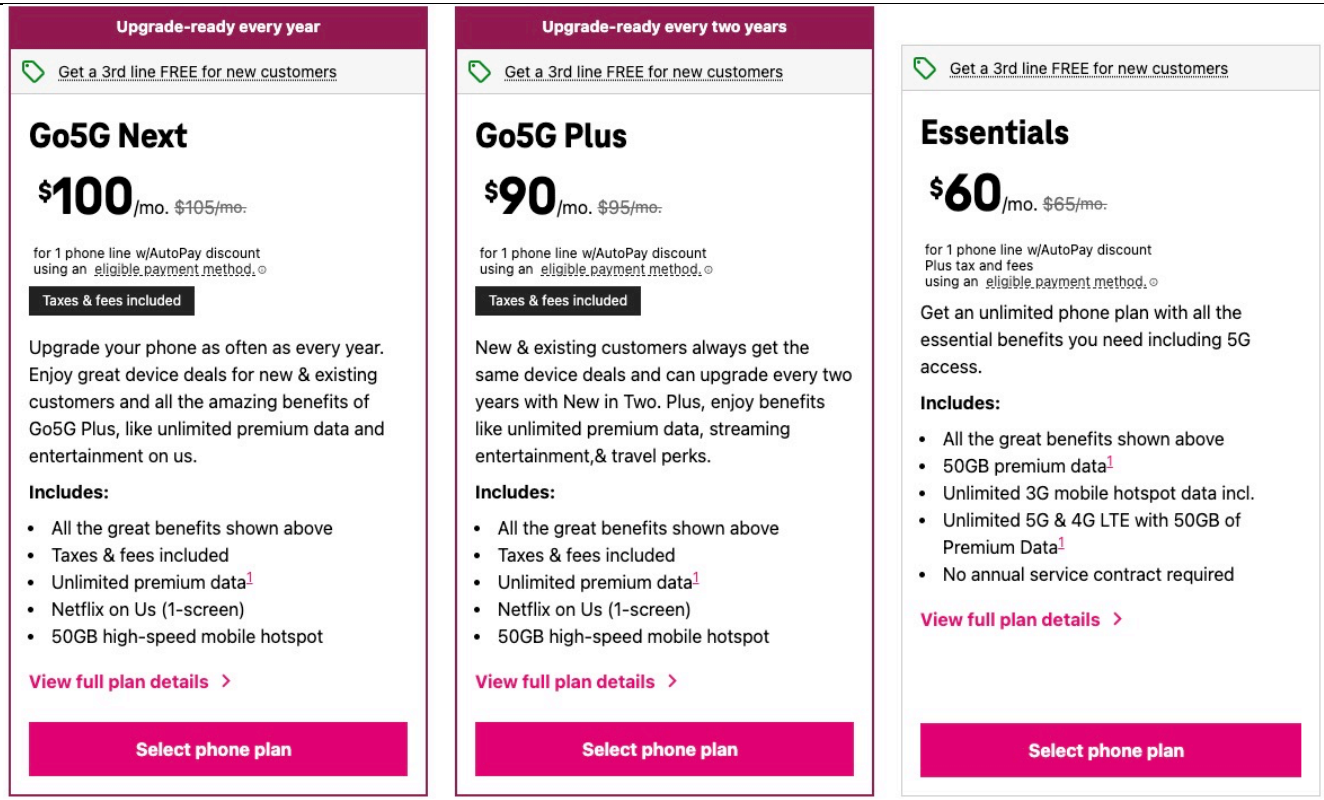


https://prepaid.t-mobile.com/plan-detail/t-mobile-prepaid-plans

	 https://www.t-mobile.com/cell-phone-plans
4. The method of claim 1, wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network.	The Accused Instrumentalities comprise sending configuration information to the wireless end-user device wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network. Mobile devices such as phones, tablets, and hotspot access points (cellular devices) which communicate with the T-Mobile wireless service network (a wireless wide-area network (WWAN)) and have a mobile hotspot feature are intermediate networking devices that forward traffic between T-Mobile's network (WWAN) and a local WiFi network (WLAN).



https://prepaid.t-mobile.com/plan-detail/t-mobile-prepaid-plans

	 https://www.t-mobile.com/cell-phone-plans
5. The method of claim 1, wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device.	The Accused Instrumentalities comprise sending configuration information to the wireless end-user device wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device. *See* claim 4; *see also, e.g.*:

Manually update your carrier settings on your iPhone or iPad

Carrier settings updates let your carrier provider update carrier network and related settings to improve cellular network connectivity and performance. Carrier settings updates can also add support for new features like 5G or Wi-Fi Calling.

When a carrier settings update is available, you'll be prompted to install it. Installation takes less than one minute, and you can keep using your device normally. If your carrier releases a mandatory update, you'll see an OK button instead of an Update button to let you know that the update was downloaded and installed.

https://support.apple.com/en-us/HT201270

Carrier Configuration

Android 6.0 and higher include a capability for privileged apps to provide carrier-specific configuration to the platform. This functionality, based on the UICC Carrier Privileges introduced in Android 5.1 (Lollipop MR1), allows carrier configuration to be moved away from the static configuration overlays and gives carriers and OEMs the ability to dynamically provide carrier configuration to the platform through a defined interface.

A properly signed carrier app can either be preloaded in the system image, installed automatically, or manually installed through an app store. The app is queried by the platform to provide configuration for settings including:

- Roaming/nonroaming networks
- Visual voicemail
- SMS/MMS network settings
- VoLTE/IMS configurations

Note: This app must be signed with the certificate that has a matching signature to one on the SIM. See How is privilege granted to a carrier app for details.

https://source.android.com/docs/core/connect/carrier

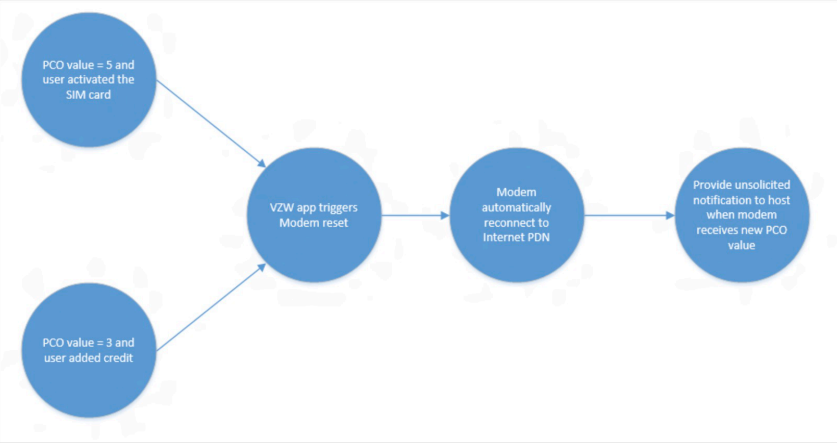
Resetting the modem based on PCO values

Based on PCO values received from the network, the modem will be reset in the following scenarios:

- The user completed self-activation after receiving PCO = 5 from the network. A new PCO value (3, 0 or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App.
- The user added more credit to their account after receiving PCO = 3. A new PCO value (0, or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App.

The host is not aware of the modem being reset, so the activated connections from the host will not be deactivated and the modem should automatically re-establish connection with those PDN after resetting. Upon establishing connection and receiving a new incoming PCO value from the network, the modem will provide an unsolicited NDIS_STATUS_WWAN_PCO_STATUS notification to the host.

The following diagram illustrates the modem's reset flow when one of these scenarios occurs, with Verizon Wireless as the example MO:



https://learn.microsoft.com/en-us/windows-hardware/drivers/network/mb-protocol-configuration-options-pco-operations

As another example, the Accused Instrumentalities comprise sending configuration information to the wireless end-user device wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device. *See* claim 4; *see also, e.g.*:

About Bluetooth, Wi-Fi, and cellular on your Apple Watch

Learn about Bluetooth and Wi-Fi for your Apple Watch and how your watch uses both. And learn how cellular on GPS + Cellular models fits in.

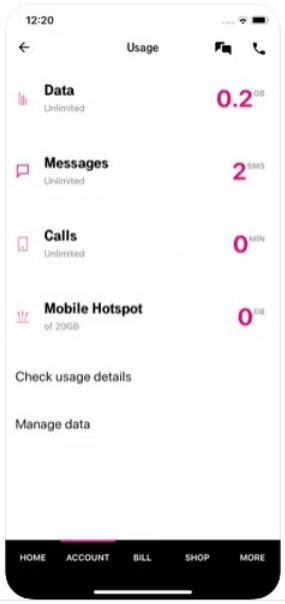
To enjoy every feature on your Apple Watch, you need to turn on Wi-Fi and Bluetooth on your paired iPhone. Open Control Center on your iPhone, then make sure that Wi-Fi and Bluetooth are on.

Your Apple Watch uses Wi-Fi and Bluetooth to communicate with your paired iPhone. If you have cellular, your watch can also stay connected through a cellular network. Your watch switches between these intelligently to choose the most power-efficient connection. Here's how:

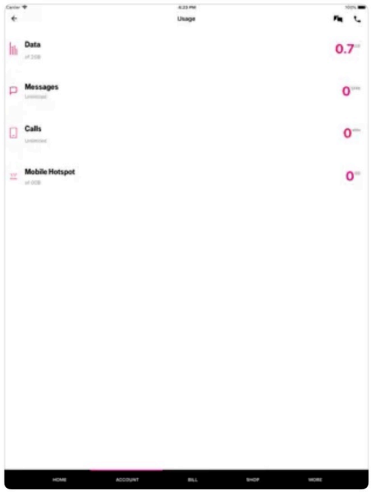
- Your Apple Watch uses Bluetooth when your iPhone is near, which conserves power.
- If Bluetooth isn't available, your Apple Watch will try to use Wi-Fi. For example, if compatible Wi-Fi is available and your iPhone isn't in Bluetooth range, your Apple Watch uses Wi-Fi.
- If Bluetooth and Wi-Fi aren't available, and you set up a cellular plan, cellular models of Apple Watch can connect to cellular networks.

https://support.apple.com/en-us/HT204562

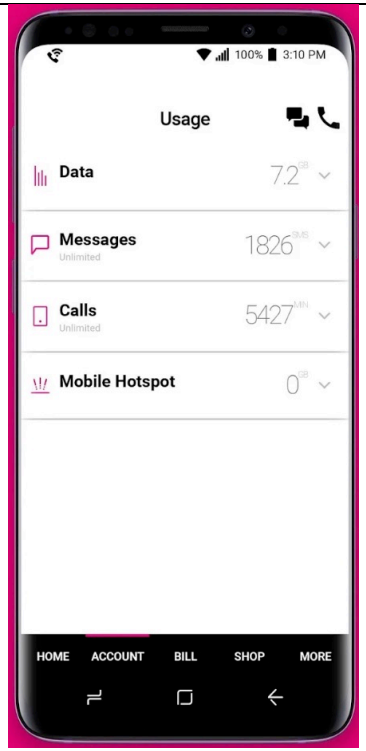
	3. Select your plan and activate cellular service. When you pair a new watch with the Galaxy Wearable app, you will be asked to select a T-Mobile plan to use with it. 1. Select **Set up a mobile plan** in the Galaxy Wearable App (if you choose to skip this step, you can set up cellular later in the Galaxy Wearable app by selecting **Watch Settings > Mobile Plans**). 2. Verify your T-Mobile account (if you're setting up for yourself, you will be asked to verify the last 4 digits of the primary account holder's SSN). 3. Choose your plan and select **Continue**. 4. Move to the bottom of the service agreement to accept, then select **Continue**. 5. Select **Use Plan** to download the eSIM Profile on your watch. https://www.t-mobile.com/support/smartwatches/samsung
6. The method of claim 1, further comprising: obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and based on the service usage measure, taking an action.	The Accused Instrumentalities comprise obtaining a service usage measure that includes a measure of service usage activity, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and based on the service usage measure, taking an action. On information and belief, the Accused Instrumentalities obtain a service usage measure accounting for communications associated with the mobile device over T-Mobile's wireless access network, including a measure of service usage activity such as information indicating overall cellular data usage and mobile hotspot data usage for the service period. Based on the service usage measure, the Accused Instrumentalities take an action such as sending configuration information that modifies a policy setting to allow, block or throttle cellular data usage or mobile hotspot data usage. *See* claim 1. *See also, e.g.*:



https://apps.apple.com/us/app/t-mobile/id561625752?platform=iphone



https://apps.apple.com/us/app/t-mobile/id561625752?platform=ipad

	 https://play.google.com/store/apps/details?id=com.tmobile.pr.mytmobile&&pli=1
7. The method of claim 6, wherein the service usage measure comprises a measure of a service usage activity.	The Accused Instrumentalities comprise obtaining a service usage measure that includes a measure of service usage activity, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and based on the service usage measure, taking an action. On information and belief, the Accused Instrumentalities obtain a service usage measure accounting for communications associated with the mobile device over T-Mobile's wireless access network, including a measure of service usage activity such as information indicating overall cellular data usage and mobile hotspot data usage for the service period. Based on the service usage measure, the Accused Instrumentalities take an action such as sending configuration information that modifies a policy setting to allow, block or throttle cellular data usage or mobile hotspot data usage. *See* claim 6.

8. The method of claim 6, wherein the action is to verify the service usage measure.	The Accused Instrumentalities comprise obtaining a service usage measure that includes a measure of service usage activity, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and based on the service usage measure, taking an action, wherein the action is to verify the service usage measure. On information and belief, based on the service usage measure indicating overall cellular data usage and mobile hotspot data usage for the service period, the Accused Instrumentalities verify the service usage measure to ensure that it accounts for the actual service usage of the mobile device. *See* claim 6.
9. The method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device.	The Accused Instrumentalities comprise obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and based on the service usage measure, taking an action to quarantine or suspend the wireless end-user device. On information and belief, the Accused Instrumentalities obtain a service usage measure indicating a prohibited service usage activity under T-Mobile's Acceptable Use Policy, and based on the service measure, quarantine or suspend the mobile device. *See, e.g.*: **CAN T-MOBILE CHANGE, SUSPEND OR TERMINATE MY SERVICES OR THIS AGREEMENT?** Yes. Except as described below for Rate Plans with the price-lock guarantee (including the "Un-Contract Promise"), we may change, limit, suspend or terminate your Service or this Agreement at any time, including if you engage in any of the prohibited uses described in these T&Cs, no longer reside in a T-Mobile-owned network coverage area, or engage in harassing, threatening, abusive or offensive behavior. If your Service, Product, or account is limited, suspended, or terminated and then reinstated, you may be charged a reconnection fee. Your account may still accrue charges even if the Service is suspended. You are responsible for any charges that are incurred while your Service or account is suspended. Under certain limited circumstances, we may also block your Device from working on our network. If the change to your Service, Product, or Rate Plan will have a material adverse effect on you, we will provide 14 days' notice of the change. You'll agree to any change by using your Service or Product after the effective date of the change. We may exclude certain types of calls, messages or sessions (e.g. conference and chat lines, broadcast, international, 900 or 976 calls, etc.), in our sole discretion, without further notice. For information about our unlocking policy, visit www.t-mobile.com/responsibility/consumer-info/policies/sim-unlock-policy.

Unless explicitly permitted by your Rate Plan or Data Plan, you are not permitted to use your Device or the Services in a way that we determine:

- Uses a repeater or signal booster other than one we provide to you;
- Compromises network security or capacity, degrades network performance, uses malicious software or "malware", hinders other customers' access to the network, or otherwise adversely impacts network service levels or legitimate data flows;
- Uses applications that automatically consume unreasonable amounts of available network capacity;
- Uses applications which are designed for unattended use, automatic data feeds, automated machine-to-machine connections, or applications that are used in a way that degrades network capacity or functionality;
- Misuses the Service, including "spamming" or sending abusive, unsolicited, or other mass automated communications;
- Accesses the accounts of others without authority;
- Results in more than 50% of your voice and/or data usage being Off-Net (i.e., connected to another provider's network) for any 2 billing cycles within any 12-month period;
- Results in unusually high usage (meeting the definition of a heavy data user for your Rate Plan) and the majority of your data usage being Smartphone Mobile HotSpot (tethering) usage for any 3 billing cycles within any 6-month period;
- Uses a fixed wireless device (provided for use in a fixed location) at a location or address other than the one provided at activation;
- Resells the Service, either alone or as part of any other good or service;
- Tampers with, reprograms, alters, or otherwise modifies your Device to circumvent any of our policies or violate anyone's intellectual property rights;
- Causes harm or adversely affects us, the network, our customers, employees, business, or any other person;
- Conflicts with applicable law;
- Is not in accordance with these T&Cs; or
- Attempts or assists or facilitates anyone else in any of the above activities.

https://www.t-mobile.com/responsibility/legal/terms-and-conditions

Other network management

If you use your data plan in a manner that could interfere with other customers' service, affect our ability to allocate network capacity among customers, or degrade service quality for other customers, we may suspend, terminate, or restrict your data session, or switch you to a more appropriate data plan, or terminate your service.

https://www.t-mobile.com/responsibility/consumer-info/policies/internet-service

12. The method of claim 1, wherein the configuration information comprises at least a portion of the service profile.	The Accused Instrumentalities comprise sending the configuration information, wherein the configuration information comprises a portion of the service profile stored in an encrypted partition of the device or in an encrypted SIM card. *See* claim 1.
13. The method of claim 1, wherein the service control link is secured by an encryption protocol.	The Accused Instrumentalities comprise sending configuration information over the service control link, wherein the service control link is secured by an encryption protocol. 4.4.4 Integrity protection of NAS signalling messages 4.4.4.1 General For the UE, integrity protected signalling is mandatory for the NAS messages once a valid EPS security context exists and has been taken into use. For the network, integrity protected signalling is mandatory for the NAS messages once a secure exchange of NAS messages has been established for the NAS signalling connection. Integrity protection of all NAS signalling messages is the responsibility of the NAS. It is the network which activates integrity protection. 4.4.4.3 Integrity checking of NAS signalling messages in the MME Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the MME or forwarded to the ESM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection: - EMM messages: - ATTACH REQUEST;

6.1.1 General

This clause describes the procedures used for EPS session management (ESM) at the radio interface (reference point "LTE-Uu").

The main function of the ESM sublayer is to support the EPS bearer context handling in the UE and in the MME.

The ESM comprises procedures for:

- the activation, deactivation and modification of EPS bearer contexts;
- the request for resources (IP connectivity to a PDN or dedicated bearer resources) by the UE; and
- the transport of user data via the control plane between the UE and the MME.

Each EPS bearer context represents an EPS bearer between the UE and a PDN. EPS bearer contexts can remain activated even if the radio and S1 bearers constituting the corresponding EPS bearers between UE and MME are temporarily released.

An EPS bearer context can be either a default bearer context or a dedicated bearer context.

A default EPS bearer context is activated when the UE requests a connection to a PDN.

Generally, ESM procedures can be performed only if an EMM context has been established between the UE and the MME, and the secure exchange of NAS messages has been initiated by the MME by use of the EMM procedures described in clause 5. The first default EPS bearer context, however, can be activated during the EPS attach procedure (see subclause 4.2). Once the UE is successfully attached, and the first default EPS bearer context has been activated during or after the attach procedure, the UE can request the MME to set up connections to additional PDNs. For each additional connection, the MME will activate a separate default EPS bearer context. A default EPS bearer context remains activated throughout the lifetime of the connection to the PDN.

6.1.2 Types of ESM procedures

***

	2) Transaction related procedures: These procedures are initiated by the UE to request for resources, i.e. a new PDN connection or dedicated bearer resources, or to release these resources: - PDN connectivity procedure; - PDN disconnect procedure; - bearer resource allocation procedure; - bearer resource modification procedure. 3GPP TS 24.301 v15.03
14. The method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting.	The Accused Instrumentalities comprise receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting. *See* claim 1. *See also, e.g.*: **Manually update your carrier settings on your iPhone or iPad** Carrier settings updates let your carrier provider update carrier network and related settings to improve cellular network connectivity and performance. Carrier settings updates can also add support for new features like 5G or Wi-Fi Calling. When a carrier settings update is available, you'll be prompted to install it. Installation takes less than one minute, and you can keep using your device normally. If your carrier releases a mandatory update, you'll see an OK button instead of an Update button to let you know that the update was downloaded and installed. https://support.apple.com/en-us/HT201270

Carrier Configuration

Android 6.0 and higher include a capability for privileged apps to provide carrier-specific configuration to the platform. This functionality, based on the UICC Carrier Privileges introduced in Android 5.1 (Lollipop MR1), allows carrier configuration to be moved away from the static configuration overlays and gives carriers and OEMs the ability to dynamically provide carrier configuration to the platform through a defined interface.

A properly signed carrier app can either be preloaded in the system image, installed automatically, or manually installed through an app store. The app is queried by the platform to provide configuration for settings including:

- Roaming/nonroaming networks
- Visual voicemail
- SMS/MMS network settings
- VoLTE/IMS configurations

Note: This app must be signed with the certificate that has a matching signature to one on the SIM. See How is privilege granted to a carrier app for details.

https://source.android.com/docs/core/connect/carrier

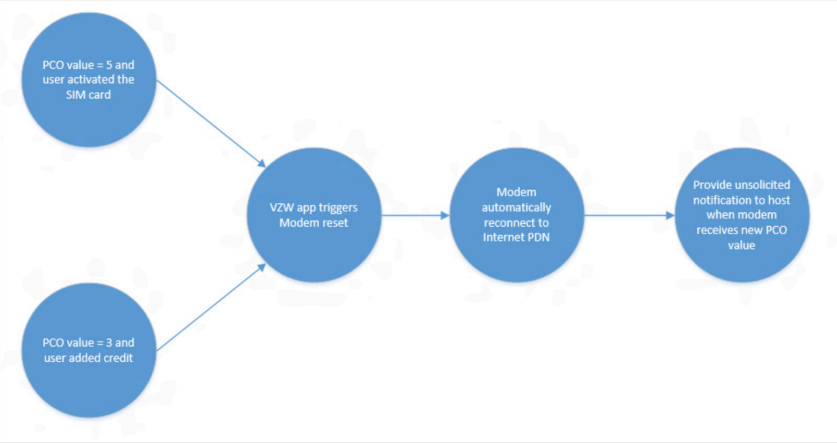
	Resetting the modem based on PCO values Based on PCO values received from the network, the modem will be reset in the following scenarios: • The user completed self-activation after receiving PCO = 5 from the network. A new PCO value (3, 0 or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App. • The user added more credit to their account after receiving PCO = 3. A new PCO value (0, or anything Mobile Operator App can recognize) will be sent to the OS and the OS will pass it to Mobile Operator App. The host is not aware of the modem being reset, so the activated connections from the host will not be deactivated and the modem should automatically re-establish connection with those PDN after resetting. Upon establishing connection and receiving a new incoming PCO value from the network, the modem will provide an unsolicited NDIS_STATUS_WWAN_PCO_STATUS notification to the host. The following diagram illustrates the modem's reset flow when one of these scenarios occurs, with Verizon Wireless as the example MO:  https://learn.microsoft.com/en-us/windows-hardware/drivers/network/mb-protocol-configuration-options-pco-operations
16. The method of claim 1, wherein the device service state comprises information associated with an encryption key.	The Accused Instrumentalities comprise receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state, wherein the device service state comprises information associated with an encryption key. *See, e.g.*:

Table 8.2.4.1: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach request message identity	Message type 9.8	M	V	1
	EPS attach type	EPS attach type 9.9.3.11	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	EPS mobile identity	EPS mobile identity 9.9.3.12	M	LV	5-12
	UE network capability	UE network capability 9.9.3.34	M	LV	3-14
	ESM message container	ESM message container 9.9.3.15	M	LV-E	5-n
19	Old P-TMSI signature	P-TMSI signature 9.9.3.26	O	TV	4
50	Additional GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
52	Last visited registered TAI	Tracking area identity 9.9.3.32	O	TV	6
5C	DRX parameter	DRX parameter 9.9.3.8	O	TV	3
31	MS network capability	MS network capability 9.9.3.20	O	TLV	4-10
13	Old location area identification	Location area identification 9.9.2.2	O	TV	6
9-	TMSI status	TMSI status 9.9.3.31	O	TV	1
11	Mobile station classmark 2	Mobile station classmark 2 9.9.2.4	O	TLV	5
20	Mobile station classmark 3	Mobile station classmark 3 9.9.2.5	O	TLV	2-34
40	Supported Codecs	Supported Codec List 9.9.2.10	O	TLV	5-n
F-	Additional update type	Additional update type 9.9.3.0B	O	TV	1
5D	Voice domain preference and UE's usage setting	Voice domain preference and UE's usage setting 9.9.3.44	O	TLV	3
D-	Device properties	Device properties 9.9.2.0A	O	TV	1
E-	Old GUTI type	GUTI type 9.9.3.45	O	TV	1
C-	MS network feature support	MS network feature support 9.9.3.20A	O	TV	1
10	TMSI based NRI container	Network resource identifier container 9.9.3.24A	O	TLV	4
6A	T3324 value	GPRS timer 2 9.9.3.16A	O	TLV	3
5E	T3412 extended value	GPRS timer 3 9.9.3.16B	O	TLV	3
6E	Extended DRX parameters	Extended DRX parameters 9.9.3.46	O	TLV	3
6F	UE additional security capability	UE additional security capability 9.9.3.53	O	TLV	6
6D	UE status	UE status 9.9.3.54	O	TLV	3
17	Additional information requested	Additional information requested 9.9.3.55	O	TV	2

Table 8.3.8.1: BEARER RESOURCE ALLOCATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource allocation request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
	Required traffic flow QoS	EPS quality of service 9.9.4.3	M	LV	2-14
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

Table 8.3.10.1: BEARER RESOURCE MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource modification request message identity	Message type 9.8	M	V	1
	EPS bearer identity for packet filter	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
5B	Required traffic flow QoS	EPS quality of service 9.9.4.3	O	TLV	3-15
58	ESM cause	ESM cause 9.9.4.4	O	TV	2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

	Table 8.3.20.1: PDN CONNECTIVITY REQUEST message content 3GPP TS 24.301 v15.03
17. The method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report.	The Accused Instrumentalities comprise receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report. *See, e.g.*:

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN connectivity request message identity	Message type 9.8	M	V	1
	Request type	Request type 9.9.4.14	M	V	1/2
	PDN type	PDN type 9.9.4.10	M	V	1/2
D-	ESM information transfer flag	ESM information transfer flag 9.9.4.5	O	TV	1
28	Access point name	Access point name 9.9.4.1	O	TLV	3-102
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538

Table 8.2.4.1: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach request message identity	Message type 9.8	M	V	1
	EPS attach type	EPS attach type 9.9.3.11	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	EPS mobile identity	EPS mobile identity 9.9.3.12	M	LV	5-12
	UE network capability	UE network capability 9.9.3.34	M	LV	3-14
	ESM message container	ESM message container 9.9.3.15	M	LV-E	5-n
19	Old P-TMSI signature	P-TMSI signature 9.9.3.26	O	TV	4
50	Additional GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
52	Last visited registered TAI	Tracking area identity 9.9.3.32	O	TV	6
5C	DRX parameter	DRX parameter 9.9.3.8	O	TV	3
31	MS network capability	MS network capability 9.9.3.20	O	TLV	4-10
13	Old location area identification	Location area identification 9.9.2.2	O	TV	6
9-	TMSI status	TMSI status 9.9.3.31	O	TV	1
11	Mobile station classmark 2	Mobile station classmark 2 9.9.2.4	O	TLV	5
20	Mobile station classmark 3	Mobile station classmark 3 9.9.2.5	O	TLV	2-34
40	Supported Codecs	Supported Codec List 9.9.2.10	O	TLV	5-n
F-	Additional update type	Additional update type 9.9.3.0B	O	TV	1
5D	Voice domain preference and UE's usage setting	Voice domain preference and UE's usage setting 9.9.3.44	O	TLV	3
D-	Device properties	Device properties 9.9.2.0A	O	TV	1
E-	Old GUTI type	GUTI type 9.9.3.45	O	TV	1
C-	MS network feature support	MS network feature support 9.9.3.20A	O	TV	1
10	TMSI based NRI container	Network resource identifier container 9.9.3.24A	O	TLV	4
6A	T3324 value	GPRS timer 2 9.9.3.16A	O	TLV	3
5E	T3412 extended value	GPRS timer 3 9.9.3.16B	O	TLV	3
6E	Extended DRX parameters	Extended DRX parameters 9.9.3.46	O	TLV	3
6F	UE additional security capability	UE additional security capability 9.9.3.53	O	TLV	6
6D	UE status	UE status 9.9.3.54	O	TLV	3
17	Additional information requested	Additional information requested 9.9.3.55	O	TV	2

Table 8.3.8.1: BEARER RESOURCE ALLOCATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource allocation request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
	Required traffic flow QoS	EPS quality of service 9.9.4.3	M	LV	2-14
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

Table 8.3.10.1: BEARER RESOURCE MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource modification request message identity	Message type 9.8	M	V	1
	EPS bearer identity for packet filter	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
5B	Required traffic flow QoS	EPS quality of service 9.9.4.3	O	TLV	3-15
58	ESM cause	ESM cause 9.9.4.4	O	TV	2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

	Table 8.3.20.1: PDN CONNECTIVITY REQUEST message content 3GPP TS 24.301 v15.03
18. The method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state.	The Accused Instrumentalities comprise receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state. *See, e.g.*:

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN connectivity request message identity	Message type 9.8	M	V	1
	Request type	Request type 9.9.4.14	M	V	1/2
	PDN type	PDN type 9.9.4.10	M	V	1/2
D-	ESM information transfer flag	ESM information transfer flag 9.9.4.5	O	TV	1
28	Access point name	Access point name 9.9.4.1	O	TLV	3-102
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538

Table 8.2.4.1: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach request message identity	Message type 9.8	M	V	1
	EPS attach type	EPS attach type 9.9.3.11	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	EPS mobile identity	EPS mobile identity 9.9.3.12	M	LV	5-12
	UE network capability	UE network capability 9.9.3.34	M	LV	3-14
	ESM message container	ESM message container 9.9.3.15	M	LV-E	5-n
19	Old P-TMSI signature	P-TMSI signature 9.9.3.26	O	TV	4
50	Additional GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
52	Last visited registered TAI	Tracking area identity 9.9.3.32	O	TV	6
5C	DRX parameter	DRX parameter 9.9.3.8	O	TV	3
31	MS network capability	MS network capability 9.9.3.20	O	TLV	4-10
13	Old location area identification	Location area identification 9.9.2.2	O	TV	6
9-	TMSI status	TMSI status 9.9.3.31	O	TV	1
11	Mobile station classmark 2	Mobile station classmark 2 9.9.2.4	O	TLV	5
20	Mobile station classmark 3	Mobile station classmark 3 9.9.2.5	O	TLV	2-34
40	Supported Codecs	Supported Codec List 9.9.2.10	O	TLV	5-n
F-	Additional update type	Additional update type 9.9.3.0B	O	TV	1
5D	Voice domain preference and UE's usage setting	Voice domain preference and UE's usage setting 9.9.3.44	O	TLV	3
D-	Device properties	Device properties 9.9.2.0A	O	TV	1
E-	Old GUTI type	GUTI type 9.9.3.45	O	TV	1
C-	MS network feature support	MS network feature support 9.9.3.20A	O	TV	1
10	TMSI based NRI container	Network resource identifier container 9.9.3.24A	O	TLV	4
6A	T3324 value	GPRS timer 2 9.9.3.16A	O	TLV	3
5E	T3412 extended value	GPRS timer 3 9.9.3.16B	O	TLV	3
6E	Extended DRX parameters	Extended DRX parameters 9.9.3.46	O	TLV	3
6F	UE additional security capability	UE additional security capability 9.9.3.53	O	TLV	6
6D	UE status	UE status 9.9.3.54	O	TLV	3
17	Additional information requested	Additional information requested 9.9.3.55	O	TV	2

Table 8.3.8.1: BEARER RESOURCE ALLOCATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource allocation request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
	Required traffic flow QoS	EPS quality of service 9.9.4.3	M	LV	2-14
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

Table 8.3.10.1: BEARER RESOURCE MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource modification request message identity	Message type 9.8	M	V	1
	EPS bearer identity for packet filter	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
5B	Required traffic flow QoS	EPS quality of service 9.9.4.3	O	TLV	3-15
58	ESM cause	ESM cause 9.9.4.4	O	TV	2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538
5C	Extended EPS QoS	Extended quality of service 9.9.4.30	O	TLV	12

Table 8.3.20.1: PDN CONNECTIVITY REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN connectivity request message identity	Message type 9.8	M	V	1
	Request type	Request type 9.9.4.14	M	V	1/2
	PDN type	PDN type 9.9.4.10	M	V	1/2
D-	ESM information transfer flag	ESM information transfer flag 9.9.4.5	O	TV	1
28	Access point name	Access point name 9.9.4.1	O	TLV	3-102
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253
C-	Device properties	Device properties 9.9.2.0A	O	TV	1
33	NBIFOM container	NBIFOM container 9.9.4.19	O	TLV	3-257
66	Header compression configuration	Header compression configuration 9.9.4.22	O	TLV	5-257
7B	Extended protocol configuration options	Extended protocol configuration options 9.9.4.26	O	TLV-E	4-65538

3GPP TS 24.301 v15.03